

Wprowadzenie
Jarosław Stelmach

Rozdział 1. Identyfikacja i ocena współczesnych zagrożeń dla obiektów użyteczności publicznej – panel ekspercki

Rozdział 2. Wyzwania dla bezpieczeństwa w kontekście rozwoju transportu intermodalnego i multimodalnego w Polsce

Paweł Lubiewski, Łukasz Foryś

Streszczenie

Wstęp

Kierunki rozwoju transportu intermodalnego i multimodalnego

Wyzwania w sferze bezpieczeństwa ruchu drogowego

Sieci transportowe jako element infrastruktury krytycznej

Zakończenie

Bibliografia

Challenges for safety in the context of the development of intermodal and multimodal transport in Poland

Biogram

Rozdział 3. Wyzwania w cyberprzestrzeni – dobre praktyki i rekomendacje

Maciej Marczyk

Streszczenie

Wstęp

Metody i narzędzia zwiększające bezpieczeństwo informacji w cyberprzestrzeni

Wnioski

Bibliografia

Summary

Biogram

Rozdział 4. Porównanie sprzętowych i programowych zapór sieciowych

Grzegorz Cichosz

Streszczenie

Wstęp

Zapora sieciowa

Filtry pakietów

Rodzaje filtrowania pakietów

Unified threat management (UTM)

Wirtualna sieć prywatna VPN

Firewall programowy

Wybór zapory sieciowej

Bibliografia

Comparison of hardware and software firewalls

Biogram

Rozdział 5. Zagrożenia dla infrastruktury krytycznej w zakresie cyberterroryzmu

Paulina Krawczyk

Streszczenie
Wstęp
Ochrona infrastruktury krytycznej przed zagrożeniami
Cyberterroryzm
Formy ochrony Infrastruktury krytycznej
Podsumowanie
Bibliografia
Summary
Biogram

Rozdział 6. Bezpieczeństwo fizyczne obiektów i infrastruktury rynku finansowego. Zagrożenia, rozwiązania, trendy – panel ekspercki

Rozdział 7. Cyber safe place – ochrona cyberbezpieczeństwa rynku finansowego jako zyskujące na znaczeniu zadanie Komisji Nadzoru Finansowego

Kamil Mroczka, Paweł Piekutowski

Streszczenie
Wstęp
Analiza terminów „cyberbezpieczeństwo” i „rynek finansowy”
Uwarunkowania prawne krajowego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej
Komisja Nadzoru Finansowego w systemie ochrony cyberbezpieczeństwa państwa – najważniejsze zadania i kompetencje
Działalność Zespołu CSIRT KNF w latach 2020–2021
Analiza zagrożeń i wsparcie w obsłudze incydentów bezpieczeństwa
Monitorowanie i analiza sposobów działania grup cyberprzestępczych
Monitorowanie i analiza złośliwego oprogramowania
Wymiana informacji o zagrożeniach w cyberprzestrzeni
Działania edukacyjne mające na celu poprawę świadomości użytkowników
Monitorowanie i ograniczanie kampanii phishingowych
Trusted Introducers
Podsumowanie – najważniejsze wyzwania w zakresie cyberbezpieczeństwa rynku finansowego
Bibliografia
Summary
Biogram

Rozdział 8. Wpływ wytworów kulturowych człowieka na zagrożenia terrorystyczne obiektów publicznych

Andrzej Pieczywok

Streszczenie
Wstęp
Konflikty i zagrożenia w mediach społecznościowych
Zachowania antyspołeczne

Zakończenie
Bibliografia
Summary
Biogram

Rozdział 9. Systemy antydronowe w bezpieczeństwie obiektów

Zygmunt Rafał Trzaskowski

Biogram

Rozdział 10. Entrance control jako element systemu bezpieczeństwa antyterrorystycznego obiektu

Jarosław Jaźwiński

Etapy działań
Strefy dostępu – wybór i rekomendacje
Biogram

Rozdział 11. Komunikacja, która ratuje życie! Rozwiązania interkomowe w sytuacjach kryzysowych

Leszek Schmidt

Wstęp
Dobór środków technicznych dla obiektu
Norma EN 62820 – systemy interkomowe budynku
Procedury postępowania workflow w systemach interkomowych
Przykłady rozwiązań ASBIS
Klasy zabezpieczenia GRADE
Bezpieczeństwo i wartość dodana
Biogram

Rozdział 12. Szkolenia online jako forma permanentnej edukacji pracowników z obszaru bezpieczeństwa

Marcin Kożuszek

Streszczenie
Szkolenia online jako forma kształcenia pracowników
Możliwości wykorzystania e-learningu w obszarze bezpieczeństwa
Bibliografia
Biogram